www.KnowledgeFlow.org

CYBER SAFETY TIP SHEET ONLINE BANKING

Tip: Never click a link in an email or text to access your bank's website, always go directly. Bookmark your bank's site.

To report fraud:

- antifraudcentre-centreantifraude.ca
- non-emergency line for your local police

1

Protect your account:

- Use password management best practices
- Enable Two Factor Authentication if available
- Do not use public wifi to access your bank account
- When setting up security questions, give 'fake' answers so that they can not be guessed by a fraudster
- Review your bank statements regularly

2

Protect your computer:

- Install software updates immediately
- Install anti-virus software

E-TRANSFERS

- Never send the password to an e-transfer by email or text
- Make the password something that can't be guessed
- Set up auto-deposit to receive e-transfers
- Be wary of a payment notification you were not expecting, if you suspect it is fraudulent email it to phishing@interac.ca

Info@KnowledgeFlow.org

LinkedIn.KnowledgeFlow.org

Facebook.KnowledgeFlow.org

Twitter.KnowledgeFlow.org


How to be #UnHackable: Be Secure
KnowledgeFlow.org
Password Checklist
1
2
3
4
UNIQUE
Create a different password for each account
STRONG
Long, with capitals, numbers and characters
SECURE
Store in a password manager
COMPLEX
Enable multi-factor authentication


Scam Red Flags
1
Fear, Urgency, Secrecy
2
CASE 1
EVIDENCE
Authority or Legitimacy
3
Payment (in any form)
4
DRIVER LICENSE
NAME SURNAME
Personal Information

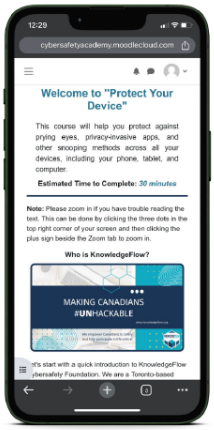
How to be #UnHackable: **Be Positive** KnowledgeFlow.org

FREE

Protect Your Device
Cybersafety for Everyone

Protect Your Information
Cybersafety for Everyone

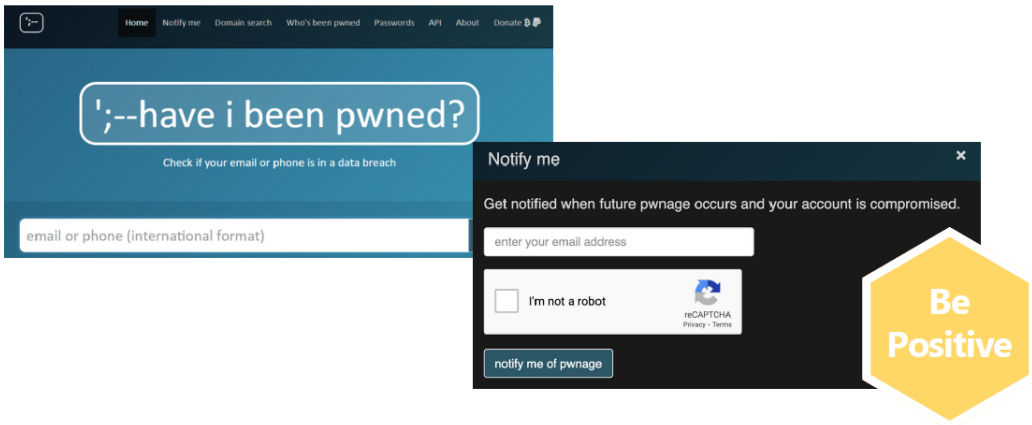
Scams: Spot Them and Stop Them
Cybersafety for Everyone



CybersafetyAcademy.ca

How to be #UnHackable: **Be Positive** KnowledgeFlow.org

Get Notified



Be Positive

How to be #UnHackable: **Be Skeptical** KnowledgeFlow.org

- Use privacy tools that run in your Web browser:

Privacy Badger

ABP AdblockPlus

CleanBrowsing

Be Private

www.KnowledgeFlow.org

CYBER SAFETY TIP SHEET

WHAT TO DO AFTER IDENTITY THEFT

Found out someone's been posting with your social media account? Noticed purchases on your credit card bill that you never made?

Other possible signs of Identity Theft:

- Being denied a loan, job or rent unexpectedly
- Bills and statements don't arrive when they are supposed to
- Calls from collection agencies or creditors for an account you don't have

Regardless of how, your data, along with your identity has been stolen, what now?

Suspect a scam? Report fraud: www.antifraudcentre-centreantifraude.ca

1

Change your passwords. Never use the same password on more than one account. Enable Two Factor Authentication, and use a password manager to generate and store strong passwords.

2

Tell the financial institution, credit card issuers, and companies involved. You may need to change your account numbers, your PINs, and get new debit and credit cards.

3

Report the identity theft to the police and the CAFC. Get a copy of the police report for your records. Contact the Canadian Anti-Fraud Centre (CAFC) 1-888-495-8501 or visit www.antifraudcentre-centreantifraude.ca.

4

Cancel any missing or stolen identification documents. Cancel government-issued documents like driver's license, birth certificate, or health card. Contact Service Ontario at **1-800-267-8097**
For SIN issues, contact Service Canada: **1-800-622-6232**
For Passport issues: **1-800-567-6868**

5

Contact Equifax and TransUnion. Request a copy of your credit reports and Dispute the fraudulent debt. Place a "fraud alert" on your file.
Equifax 1-800-465-7166
www.equifax.ca
TransUnion 1-800-663-9980
www.transunion.ca

Info@KnowledgeFlow.org

LinkedIn.KnowledgeFlow.org

Facebook.KnowledgeFlow.org

Twitter.KnowledgeFlow.org